



Department of Homeland Security Daily Open Source Infrastructure Report for 19 June 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The New York Times reports the first National Guard troops ordered to the United States–Mexico border as part of the plan to improve security arrived in the four border states and began their work on Sunday, June 18. (See item [10](#))
- The Department of Homeland Security issued findings on Friday, June 16, from a national assessment of the country's catastrophic planning capabilities; the Nationwide Plan Review looked at whether existing emergency operations plans for states and urban areas are sufficient for managing a catastrophic event. (See item [23](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *June 16, Standard (China)* — **Massive gas field found off Hong Kong.** China's largest offshore oil producer, CNOOC, and Husky Energy said they have discovered a deepwater gas field off Hong Kong that analysts estimate to be worth as much as US\$1.6 billion. Husky Oil China has made a "significant" discovery on block 29/26 in the Pearl River Mouth Basin, the first deepwater find off China, Husky Energy said Wednesday, June 14. The field may contain potential recoverable resources of four trillion to six trillion cubic feet of natural gas, which would make it one of the largest such discoveries offshore China, said John Lau of Husky

Energy. Production is unlikely before 2010 at the earliest, JPMorgan said. If confirmed, the discovery will add as much as seven percent to China's gas reserves.

Source: http://www.thestandard.com.hk/news_detail.asp?we_cat=2&art_id=20958&sid=8434927&con_type=1&d_str=20060616

2. *June 15, Clarion-Ledger (MS)* — **Mississippi Power plant fully restored and ready for summer.** Almost ten months after Hurricane Katrina flooded Mississippi Power's Plant Watson in Gulfport with more than 16 million gallons of water, repairs are complete and the plant is fully operational. The facility suffered significant damage from the August 29, 2005 storm. Water in the lower levels reached a depth of nearly 20 feet, according to the company. The turbine generators and boilers were not damaged, but nearly all of the electronic controls and water pumps that operate the plant's five units were affected. Company employees and outside contracting crews worked 24-hour days after the storm and restored Unit 4, a 250-megawatt coal-fired unit, to operational status within 46 days. Unit 5, a 500-megawatt coal-fired unit responsible for nearly half of the plant's output, came back in service just before the end of the year. Repairs to the plant's three smaller units, used primarily to meet summer peaking demand, were completed May 31.

Source: http://www.clarionledger.com/apps/pbcs.dll/article?AID=/2006_0615/BIZ/60615014

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

3. *June 19, Continuity Central* — **U.S. agencies provide financial institutions with hurricane-related business continuity advice.** The member agencies of the Federal Financial Institutions Examination Council and the Conference of State Bank Supervisors have announced the publication of "Lessons Learned From Hurricane Katrina: Preparing Your Institution for a Catastrophic Event." The booklet captures the experiences of various financial institutions in the aftermath of Hurricane Katrina and highlights lessons that other institutions may find helpful in considering their readiness for a future catastrophic event. Major hardships faced by these institutions included: communications outages made it difficult to locate missing personnel; lack of electrical power or fuel for generators rendered computer systems inoperable; multiple facilities were destroyed or sustained significant damage; some branches and ATMs were under water for weeks; and mail service was interrupted for months in some areas.

Lessons Learned booklet: <http://www.fdic.gov/regulations/resources/lessons/index.html>

Source: <http://continuitycentral.com/news02617.htm>

4. *June 15, Queens Chronicle (NY)* — **Radio Shack workers accused of ID theft.** Three employees at a Maspeth, NY, Radio Shack have been accused of stealing the identities of two dozen people over an eight month period last year. The employees are accused of using Radio Shack credit card accounts in other people's names to buy \$23,000 worth of merchandise. According to the District Attorney's Office, in June 2005 one of the men allowed two still unidentified individuals to open credit cards accounts at the store despite providing questionable identification. Those individuals eventually opened between 20 and 30 accounts at the store under different names, and used those accounts to buy \$40,000 in merchandise. In return, those individuals provided the three men with personal information — apparently taken from cell phone applications — that they used to open 21 separate credit card accounts themselves. The defendants allegedly used the credit cards to buy computers, cameras, and MP3 players. Allegedly, one defendant would open the account while the other would process the sales.

Source: http://www.zwire.com/site/prINTERfriendly.cfm?brd=2731&dept_id=574901&newsid=16795547

5. *June 15, CNET News* — **Online threats outpacing law crackdowns.** Authorities are cracking down on phishing and botnets, but the threats are advancing, representatives from the U.S. Department of Justice (DOJ) and the U.S. Air Force Office of Special Investigations said at the Computer Security Institute's NetSec event. Jonathan Rusch of DOJ said almost 17,500 phishing Websites were reported to the Anti-Phishing Working Group in April. Increasingly, phishers use Trojan horses that pack backdoors, screen grabbers, or keystroke loggers to capture log-in names, passwords, and other information, he said. In April, there were 180 unique examples of such malicious code. Wendi Whitmore of the Air Force Office of Special Investigations, said "Botnets are one of the greatest facilitators of cybercrime these days. Really the cybercrime arena is wrapped around botnets." Meanwhile, bot masters are getting smarter about hiding. Today, most botnets are controlled using Internet Relay Chat, or IRC, servers, and channels. Soon that could become instant messaging, peer-to-peer technology, or protocols used by Internet phone services such as Skype or Vonage, Whitmore said. Whitmore expects cybercrooks to maintain smaller botnets with the hope of staying under the radar.

Source: http://news.com.com/2102-7349_3-6084317.html?tag=st.util.pri nt

6. *June 15, Computerworld* — **Trojan horse captured data on 2,300 Oregon taxpayers from infected government PC.** The Oregon Department of Revenue has been contacting some 2,300 taxpayers to notify them that their names, addresses, and Social Security numbers may have been stolen by a Trojan horse program downloaded accidentally by a former worker who was surfing pornographic sites while at work in January. Agency spokesperson Rosemary Hardin said the malware was discovered on the worker's desktop computer on May 15, after the worker was fired for inappropriate Web surfing. The malicious program was designed to capture keystrokes on the former employee's computer, Hardin said. The employee was an entry-level worker who was assigned to entering taxpayer name and address changes, as well as some Social Security numbers. "We know that the information that the Trojan gathered up was transmitted outside of the agency" to an unrelated Website. Officials at the Department of Revenue don't know whether any of the transmitted information was ever received, she said. None of the information included income tax or banking information for the affected taxpayers.

There have been no reports of identity theft connected to the incident so far, according to Hardin.

Source: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9001222>

[\[Return to top\]](#)

Transportation and Border Security Sector

7. *June 17, Washington Post* — **At border crossing, it's zero tolerance.** This year, most of the 210-mile stretch of riverbank between the small border cities of Eagle Pass and Del Rio has become a "zero tolerance zone." If apprehended by the U.S. Border Patrol, illegal immigrants are prosecuted by federal authorities for a misdemeanor, sent to jail for 15 to 180 days and then deported. If they are caught illegally entering the country a second time, they are eligible for a felony charge of illegal entry and as much as two years in federal prison. This federal experiment called "Operation Streamline II" has shown what it takes to stop the flow of illegal immigrants: aggressive enforcement of the laws on the books. That entails putting the fate of each illegal border crosser in the hands of not only the Border Patrol, but also the local offices of the U.S. attorney and the U.S. Marshals Service, the Federal Bureau of Prisons and the regional Immigration and Customs Enforcement office of the Department of Homeland Security. The coordination is complicated, and the logistics is a "headache," one federal official said. Still, this pilot project, which the Border Patrol is considering implementing along other parts of the 2,000-mile border with Mexico, has been worthwhile, officials said.

Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/06/17/AR2006061700455.html?sub=AR>

8. *June 16, Fresno Bee (CA)* — **California train wreck linked to fatigue.** Railroad signals and switching equipment were operating properly before two BNSF Railway freight trains collided early Wednesday, June 14, in Madera County, a railroad spokesperson said Thursday, June 15. While not ruling out mechanical failure, the news fueled speculation that human factors — such as employee fatigue — may have caused the wreck that injured five people, scattered rail cars and shut down one of the state's main rail lines Wednesday. A spokesperson for the rail employees union said that crewmembers may have been too tired or distracted to prevent the collision. Railroad workers can work 12 hours a day, seven days a week, with schedules changing at a moment's notice, said Tim Smith, state chairman of the legislative board of the Brotherhood of Locomotive Engineers and Trainmen in Auburn. A railroad safety expert said the northbound train had the right of way because it was already moving onto side tracks to allow the southbound train to pass. The southbound train should have stopped to allow the northbound train to finish its maneuver. Though the railroad released some findings, a spokesperson for the Federal Railroad Administration said it's too early in the investigation to determine the official cause of the collision.

Source: <http://www.fresnobee.com/local/story/12326987p-13059240c.htm>

9. *June 16, Department of Transportation* — **Funding grant for "FrontRunner" Weber County-to-Salt Lake City Commuter Rail project.** Salt Lake City area commuters got a big boost on Friday, June 16, when Department of Transportation Secretary Norman Y. Mineta sealed an agreement with the Utah Transit Authority (UTA) for \$489 million in federal funding

for the “FrontRunner” Weber County–to–Salt Lake City Commuter Rail line. The money will be used to build the new 44 mile commuter rail line that is expected to carry almost 12,000 weekday passengers taking nearly 6,000 cars off the roads everyday Mineta said during a visit to the Farmington Station construction site this afternoon. The Full Funding Grant Agreement represents the federal government,s commitment to provide funding for the project, Mineta said. The funds will be allocated over a seven–year period from 2006 through 2012. It allows construction to continue on the new commuter rail line, which will provide service from Pleasant View to the existing Salt Lake City Intermodal Terminal in downtown Salt Lake City, with stops in Salt Lake, Weber and Davis counties. The line’s downtown terminal will provide commuter rail passengers a direct connection for commuter rail, light rail, and passenger rail with UTA buses and Greyhound intercity bus service. Feeder buses will provide transportation from the terminal to local business and residential areas.

Source: <http://www.dot.gov/affairs/fta0906.htm>

10. *June 16, New York Times* — **Guard Troops begin mission on Mexican Border.** The first National Guard troops ordered to the United States–Mexico border as part of President Bush's plan to improve security arrived in the four border states and planned to begin work by Sunday, June 18. "The Jump Start operation has begun," Mario Martinez, a Border Patrol spokesperson in Washington, said Friday, June 16, using the Guard's name for the border mission. Most of the troops arrived by Thursday, June 15, to prepare for their assignments, which will include monitoring surveillance cameras and sensors, building roads, putting fencing along the border and other tasks that will free up regular Border Patrol agents to police the 2,000–mile divide between Mexico and California, Arizona, Texas, and New Mexico. Border Patrol and Guard officials said Friday that the first group of Guard members would number about 800. By August, up to 6,000 Guard members are to be assigned to the border mission. Most of the Guard members will be unarmed unless they are in a hazardous area. Much of their time will be spent in Border Patrol offices watching monitors and handling other equipment, while those in the field will alert Border Patrol agents if they see someone crossing the border illegally.

Source: <http://www.nytimes.com/2006/06/18/us/18guard.html?hp&ex=1150603200&en=27b1a1421283edca&ei=5094&partner=homepage>

11. *June 14, Reuters* — **United Airlines plans to cut jobs to save money.** UAL Corp, the parent of United Airlines, plans to slash at least 1,000 jobs by the end of this year as part of its overall goal to reduce costs by \$400 million, its chief executive said on Wednesday, June 14. United plans to eliminate salaried and management positions as part of its plan to reduce \$100 million in general and administrative expenses, Chief Executive Glenn Tilton said at the Merrill Lynch Global Transportation conference. Other components of the \$400 million cut include reducing purchased services costs by \$200 million, slashing marketing costs by \$60 million, and saving \$40 million from increased operational efficiencies.

Source: http://money.cnn.com/2006/06/14/news/companies/united_airlin.es.reut/index.htm?cnn=yes

[[Return to top](#)]

Postal and Shipping Sector

12.

June 16, DMNews — **USPS generates net income of \$103 million in April.** The U.S. Postal Service (USPS) generated net income of \$103 million before escrow allocation during April, according to financial and operating statements. Contributing to the performance was the new postage rate structure implemented January 8, which provided a 5.4 percent revenue increase, needed to fulfill the Postal Civil Service Retirement System Funding Act. After the escrow allocation, USPS' financial position for April shifts to a net deficiency of \$147 million. Total mail volume in April was 1.9 percent less than last year, and mail volumes in all major mail categories were below April 2005 levels. The Civil Service Retirement System Funding Act required the USPS to place \$3 billion in an escrow account by September 30, 2006, to cover the difference between the retirement costs before and after the law's implementation. The USPS said it is allocating \$250 million monthly for purposes of reconciling its financial position. Source: <http://www.dmnews.com/cms/dm-news/direct-mail/37096.html>

[[Return to top](#)]

Agriculture Sector

13. *June 16, Stop Soybean Rust News* — **First rust on soybeans this year found in southeast Florida.** Florida officials have confirmed Asian soybean rust in three maturity groups of soybeans in a sentinel plot in Martin County. This is the first occurrence of soybean rust on soybeans planted this season anywhere in the U.S. Carrie Harmon of the University of Florida said there was a 29 percent incidence of rust in the plot, with the oldest infection being in the Group III soybeans. She said it then spread to the Group V and then the Group VII in a pattern similar to that seen in plots last year. The samples were collected by a scout Thursday, June 15, in the sentinel plot near West Palm Beach, Fla., and, since this is the first time for rust in this southeastern-Florida county. Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=852>

14. *June 15, Minnesota Board of Animal Health* — **Anthrax in Minnesota cattle herds.** Over the weekend of June 10 and 11, five cows and one bull were found dead in a Kittson, MN, beef herd. A blood sample was collected and sent to the North Dakota State University Veterinary Diagnostic Laboratory in Fargo, ND. On June 14, the Board received confirmation from the lab that the sample was positive for the disease. The herd had not been vaccinated for anthrax. The bacteria that causes anthrax, *Bacillus anthracis*, is naturally occurring throughout the U.S. Anthrax spores in the soil can become active following flooding and subsequent drought, posing a risk to grazing livestock. Grazing animals are most likely to become infected with anthrax in the summer after periods of heavy rain, flooding, or excavation. Source: http://www.bah.state.mn.us/diseases/anthrax/anthrax_prgm.htm

[[Return to top](#)]

Food Sector

15. *June 16, Reuters* — **Infected feed likely cause of Canada mad cow case.** An official probe into Canada's latest case of mad cow disease — an animal detected with the bovine spongiform encephalopathy disease on April 16, 2006 — found that contaminated feed was the likely

source of the infection, the Canadian Food Inspection Agency said on Friday, June 16. "While a specific source of infection was not found, investigators determined that vehicles and equipment used to ship and receive a variety of ingredients likely contaminated cattle feed with the disease agent," the agency said.

Source: http://today.reuters.com/news/newsArticle.aspx?type=healthNews&storyID=2006-06-16T182036Z_01_N16245681_RTRUKOC_0_US-FOOD-CANADA-BSE.xml&archived=False

- 16. June 15, Food Safety and Inspection Service — Outreach sessions for small and very small plants announced.** Small and very small plant owners and operators are invited to join Food Safety and Inspection Service (FSIS) personnel at outreach sessions to bring industry and inspection personnel together to promote a uniform understanding of the regulations. As part of the initiative to enhance outreach to assist small and very small plants, FSIS is holding a series of outreach sessions. The sessions will cover a regulatory walk through of the Sanitation standard operating procedures and Rules of Practice requirements.

Source: http://www.fsis.usda.gov/News_&_Events/Outreach_Sessions_SVS_Plants/index.asp

[\[Return to top\]](#)

Water Sector

- 17. June 16, Associated Press — China builds dams to slow toxic spill.** Chinese authorities tried to slow the spread of a toxic spill by building 51 makeshift dams along the tainted river and using fire trucks to pump out polluted water before it reaches a reservoir serving a city of 10 million people, state media said Friday, June 16. The spill of 60 tons of coal tar into the Dasha River in north China's Shanxi province was the latest in a series of mishaps fouling the country's already polluted waterways. Officials said there have been at least 76 water pollution accidents in the last six months.

Source: <http://www.breitbart.com/news/2006/06/16/D8I9BVQO0.html>

- 18. June 16, Associated Press — Water executives accused of hiding radium.** Two former managers at a United Water subsidiary in Toms River, NJ, were indicted by a state grand jury on Thursday, June 15, on charges that they manipulated tests to hide high levels of radium in the drinking water of a community where environmental officials have linked contaminated water to childhood cancer. George Flegal, the former general manager for United Water Toms River, and Richard Ottens Jr., the former operations manager, were accused of shutting down one of the wells that supplied the company's water during a test for radioactive materials. The September 12, 2005 test showed the water system was within the legal limit for radium. But, in fact, the amount of radium exceeded allowable amounts, officials say. United Water Toms River, a subsidiary of Harrington Park-based United Water, serves 122,000 people in a portion of Ocean County.

Source: <http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnFIZUVFeXk1JmZnYmVsN2Y3dnFIZUVFeXk2OTQ0ODE5JnlvaXJ5N2Y3MTdmN3ZxZWVFRXl5Mg==>

[\[Return to top\]](#)

Public Health Sector

19. *June 16, Associated Press* — **Iowa mumps outbreak appears to be contained.** The number of mumps cases in Iowa has declined dramatically over the past few weeks, and the outbreak appears to be contained, state public health officials said Friday, June 16. They credit the state's intensive immunization campaign that started in April and efforts to inform the public. The U.S. Centers for Disease Control and Prevention (CDC) and a drug company have been providing extra vaccine in an effort to get Iowans immunized with the two recommended doses. Even with the recommended immunizations, about 10 percent of the population remains susceptible to the illness. As of Wednesday, June 14, there were 1,938 confirmed and probable cases of mumps reported by the Iowa Department of Public Health. The CDC has said there have been more than 3,200 mumps cases reported in 12 states, with Iowa the hardest hit.

Mumps information: <http://www.cdc.gov/nip/diseases/mumps/default.htm>

Source: http://www.globegazette.com/articles/2006/06/16/latest_news/doc4493685a23516280862920.txt

20. *June 16, Reuters* — **Nigeria changes tack to halt polio surge.** Nigeria is trying a new, more comprehensive immunization strategy to reverse a surge in polio infections that threatens global efforts to wipe out the disease. Nigeria has recorded 467 new cases of polio so far this year, compared with 224 for the whole of last year, according to the latest figures from the National Program on Immunization (NPI). Nigeria is under pressure to act after World Health Organization (WHO) members singled it out in May as the only part of the world where the virus thrives. Five northern states in Nigeria account for around 70 percent of cases worldwide. The NPI has struggled to reverse the effects of a year-long ban on polio vaccinations launched in mid-2003 by predominantly Muslim northern states over allegations that the vaccines were contaminated to spread sterility and HIV and AIDS among Muslims. The ban caused a dramatic increase in polio infections and the virus spread from northern Nigeria to many other countries. After the ban was lifted, the NPI launched a series of vaccination campaigns that reduced infection rates in 2005. The new strategy called "Immunization Plus", which involves delivering the oral polio vaccine as part of a package including measles and diphtheria, pertussis, tetanus vaccines.

Global Polio Eradication Initiative: <http://www.polioeradication.org/>

Source: http://www.iol.co.za/index.php?set_id=1&click_id=86&art_id=qw1150456320935B243

21. *June 16, Agence France-Presse* — **Bird flu virus confirmed in large Hungarian poultry farm.** The H5N1 bird flu strain has been confirmed for the first time in a large poultry rearing region of Hungary by a European Union (EU) laboratory, veterinary officials said Friday, June 16. The H5 virus, which is not highly pathogenic, had been detected by Hungarian authorities in the southeastern region of Kiskunmajsa on June 9. But the EU's reference laboratory in Weybridge, England, confirmed that the virus affecting geese and ducks belonged to the H5N1 strain, Hungary's chief veterinarian Miklos Suth said. Some 2,300 poultry have died at the poultry farm in Kiskunmajsa. About 500,000 other poultry have been slaughtered as a precautionary measure.

Source: http://news.yahoo.com/s/afp/20060616/hl_afp/healthfluhungary_060616202824;_ylt=AuPAEoGKH8Cy3wlSnRqIdyuJOrgF:_ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

[\[Return to top\]](#)

Government Sector

Nothing to report.

[\[Return to top\]](#)

Emergency Services Sector

22. *June 17, Agence France–Presse* — **Police launch eye–in–the–sky technology above Los Angeles.** The Los Angeles County Sheriff's Department is testing an unmanned aerial vehicle above Los Angeles. Police say the drone, called the SkySeer, will be able to accomplish tasks too dangerous for officers and free up helicopters for other missions. "This technology could be used to find missing children, search for lost hikers, or survey a fire zone," said Commander Sid Heal, head of the Technology Exploration Project of the Los Angeles County Sheriff's Department. The drone comes equipped with low–light and infrared capabilities and can fly at speeds up to 30 miles per hour for 70 minutes. A small camera capable of tilt and pan operations is fixed to the underside of the drone which sends the video directly to a laptop command station.

Source: <http://www.breitbart.com/news/2006/06/17/060617210138.lttks6 7y.html>

23. *June 16, Department of Homeland Security* — **DHS releases review of nationwide catastrophic event preparedness.** The Department of Homeland Security (DHS) issued findings Friday, June 16, from a national assessment of the country's catastrophic planning capabilities. Responding to directives from President Bush and the Congress, following Hurricane Katrina, the Nationwide Plan Review looked at whether existing emergency operations plans for states and urban areas are sufficient for managing a catastrophic event. The Review also presents conclusions on actions needed by the federal government to improve and coordinate planning. Conducted in all 56 States and territories and 75 urban areas over six months, the Nationwide Plan Review was the most comprehensive assessment of emergency operations plans to date relative to planning for a catastrophic event. Reviewers examined nearly 2,800 emergency operations plans and related documents with participation from more than 1,000 emergency managers and homeland security officials. The National Plan Review findings demonstrate the need for all levels of government across the country to improve emergency operations plans for catastrophic events such as a major terrorist attack or category–five hurricane strike. After completing the assessments and findings, the reviewers also provided more detailed follow–up briefings to individual States and urban areas.

Fact Sheet – Nationwide Plan Review:

http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0928.xml

Fact Sheet – Nationwide Plan Review Initial Conclusions:

http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0929.xml

Nationwide Plan Review (PDF):

http://www.dhs.gov/interweb/assetlibrary/Prep_NationwidePlan_Review.pdf

Source: <http://www.dhs.gov/dhspublic/display?content=5695>

24. *June 16, Federal Emergency Management Agency* — Is your business ready for a disaster?

When disaster strikes, businesses can be affected too. According to disaster recovery officials, preparing for a disaster, and mitigating the damage a business most likely would suffer, is something every company should do. There are four critical parts to disaster preparation: making the company's physical location less vulnerable, ensuring that business data such as sales records, customer lists, tax information, etc. is backed up offsite, purchasing adequate insurance coverage, and formulating a contingency plan to continue operating even if the company's location is heavily damaged or destroyed.

Source: <http://www.fema.gov/news/newsrelease.fema?id=27079>

25. *June 16, Post–Searchlight (GA)* — Mock tornado drill held at college. Local emergency response leaders all agreed a mock tornado drill held at Bainbridge College in Bainbridge, GA, went smoothly and was beneficial to those who took part. Shortly after 9 a.m. Thursday, June 15, E–911 dispatchers relayed a report that a tornado had touched down in two places and many people were injured, which began a drill to test the response of police, firefighters and emergency medical personnel to a disaster situation. An emergency command center was set up, which followed the protocol of the U.S. Homeland Security's National Incident Management System. Police used a common radio frequency to aid in communication. Jan Godwin, director of public relations for Memorial Hospital, issued a report of imaginary casualties associated with the tornado drill. Forty–seven people were brought to the hospital. Source: http://www.zwire.com/site/news.cfm?newsid=16802421&BRD=2068&PAG=461&dept_id=387468&rft=6

[[Return to top](#)]

Information Technology and Telecommunications Sector

26. *June 16, US–CERT* — Technical Cyber Security Alert TA06–167A: Microsoft Excel Vulnerability. Microsoft Excel contains an unspecified vulnerability. Opening a specially crafted Excel document, including documents hosted on Websites or attached to email messages, could trigger the vulnerability. Office documents can contain embedded objects. For example, a malicious Excel document could be embedded in an Word or PowerPoint document. Office documents other than Excel documents could be used as attack vectors. At the time of writing, there is no complete solution available. For more information, please see Vulnerability Note VU#802324: <http://www.kb.cert.org/vuls/id/802324>
Source: <http://www.us-cert.gov/cas/techalerts/TA06–167A.html>

27. *June 13, TechSpot* — Spyware attacks tripled last year. New research conducted by security company Aladdin's Content Security Response Team finds that the amount of spyware detected on the Internet is booming. The construction of spyware and Trojans now dominates malware production, with malware authors shifting their attention away from traditional computer viruses. Aladdin's report found that the number of malicious threats rose from 1,083 in 2004 to 3,389 in 2005. This represents a massive increase of more than 213 percent. Trojans grew from 1,455 in 2004 to 3,521 in 2005, which is a 142 percent rise. Shimon Gruper, vice president of technologies for the Aladdin eSafe Business Unit believes that this represents a fundamental shift for many criminals away from traditional crimes and into computer crime.

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT reports that Microsoft has released updates that address critical vulnerabilities in Microsoft Windows, Word, PowerPoint, Media Player, Internet Explorer, and Exchange Server. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service on a vulnerable system.

Microsoft Security Bulletin Summary for June 2006 addresses vulnerabilities in Microsoft Windows, Word, PowerPoint, Media Player, Internet Explorer, and Exchange Server. <http://www.microsoft.com/technet/security/bulletin/ms06-jun.mspx>

Please review the US-CERT National Cyber Alert System / Current Activity / Vulnerability Resources web page: <http://www.us-cert.gov/>

Vulnerability in Symantec AntiVirus Software

US-CERT is aware of a buffer overflow vulnerability in Symantec Client Security and Symantec Antivirus Corporate Edition. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. We are not aware of any public exploits at this time. For more information please review the following:

VU#404910 – Symantec products vulnerable to buffer overflow:
<http://www.kb.cert.org/vuls/id/4049100>

Symantec Advisory SYM06-010 – Symantec Client Security and Symantec AntiVirus Elevation of Privilege:
<http://securityresponse.symantec.com/avcenter/security/Content/2006.05.25.html>

US-CERT will advise as more information becomes available.

PHISHING SCAMS

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing

incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 4672 (eMule), 6881 (bittorrent), 38566 (----), 445 (microsoft-ds), 24232 (----), 32790 (----), 25 (smtp), 135 (epmap), 113 (auth) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

28. *June 18, Associated Press* — Immigration costs strain national parks. Drug smugglers fleeing Mexican police crossed into the Organ Pipe Cactus National Monument desert park and fatally shot a ranger four years ago, prompting officials to build a 30-mile vehicle barrier. That steel-and-concrete wall stops most cars from speeding in from Mexico. But drug and human traffickers have switched to rural entryways into Arizona. Thousands of people now cross on foot. They leave piles of trash, build fires, damage the park's famous cacti, and create countless trails through the fragile desert vegetation. Park workers spend most of their time backing up Border Patrol officers and dealing with border issues. The problems are not just on the border. After the attacks of September 11, 2001, the government added new homeland security responsibilities at national icons such as the Washington Monument, Independence Hall, and Mount Rushmore. Since 2001, the Park Service has received an additional \$35 million in annual money for such duties. The government also provided \$91 million in one-time dollars for icon parks and \$18 million for Organ Pipe's barrier. Homeland security, such as increased protections from illegal immigration, is "a newly identified priority," said Department of the Interior Deputy Secretary Lynn Scarlett.

Source: http://www.boston.com/news/nation/articles/2006/06/18/immigration_costs_strain_national_parks/

29. *June 16, Baltimore Sun* — Man shot in Maryland movie theater. Baltimore County police have identified a man who was fatally shot inside a movie theater at an Owings Mills shopping center Thursday night, June 15, in a bizarre incident that police described as a random attack. Paul Schrum, 62, of Pikesville, MD, died from bullet wounds to the head and upper body, authorities said on Friday, June 16. The shooter, Mujtaba Rabbani Jabbar, 24, of Owings Mills, MD, was arrested at the scene. He has been charged with first-degree murder and handgun use in commission of a violent crime. According to authorities, immediately after the shooting, Jabbar walked up to a counter in the lobby where the theater manager was seated, placed the

gun on the counter and said, "I just shot someone."

Source: http://www.baltimoresun.com/news/local/baltimore_county/bal-movie0616.0.1777900.story?coll=bal-home-headlines

[[Return to top](#)]

General Sector

30. *June 18, Associated Press* — Book: al Qaeda planned gas attack on New York subways.

U.S. officials received intelligence that al Qaeda operatives had been 45 days away from releasing a deadly gas into the city's subways when the plan was called off by Osama bin Laden's deputy in 2003, according to a book excerpt released Sunday, June 18, on Time magazine's Website. According to the investigative report by Ron Suskind, an informant close to al Qaeda leaders told U.S. officials that Ayman al-Zawahri had canceled the plan in January 2003, despite the likelihood that the strike would have killed as many people as the September 11 attacks. The informant said the operatives had planned to use a small, easily concealed device to release hydrogen cyanide into multiple subway cars. U.S. officials had already discovered plans for the device on the hard drive of a computer of a Bahraini jihadist arrested in February 2003, and they had been able to construct a working model from the plans. A New York Police Department spokesperson said authorities had known of the planned attack. "We were aware of the plot and took appropriate precaution," Paul Browne said.

Source: http://www.usatoday.com/news/nation/2006-06-18-subway-plot_x.htm

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website:

<http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.